Evaluation Policy

**Purpose:**

[Insert Covered Entity or Business Associate name] is committed to conducting business in compliance with all applicable laws, regulations and policies. [Insert Covered Entity or Business Associate name] has adopted this policy to ensure that its Security and Privacy Policies are up to date and effective in ensuring the confidentiality, integrity and availability of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) created, received, maintained and transmitted by [Insert Covered Entity or Business Associate name]. Periodic HIPAA policy evaluations are important for ensuring continued legal compliance.

**Policy:**

1. Initial Evaluation
   1. [Insert Covered Entity or Business Associate name] Security or Privacy Policies or Procedures will be evaluated initially to determine their compliance with the Security or Privacy Regulations.
   2. Once compliance with the Security or Privacy Regulations is established, the [Insert Covered Entity or Business Associate name] Security or Privacy Policies or Procedures will be evaluated on a periodic basis (Insert chosen periodic basis- annually is recommended) to assure continued viability in light of technological, environmental or operational changes that could affect the security of PHI and ePHI.
2. Periodic Evaluation by [Insert Covered Entity or Business Associate name] Information Security Officer
   1. The Information Security Officer will review on an on-going basis the viability of [Insert Covered Entity or Business Associate name] Security Policies and general approaches taken by Departments in their Security Procedures.
   2. The Information Security Officer will develop and recommend to [Insert Covered Entity or Business Associate name] any necessary Security Policy or Procedure changes.
3. Periodic Evaluation by [Insert Covered Entity or Business Associate name] Information Privacy Officer
   1. The Information Privacy Officer will review on an ongoing basis the viability of [Insert Covered Entity or Business Associate name] Privacy Policies and general approaches taken by Departments in their Privacy Procedures.
   2. The Information Privacy Officer will develop and recommend to [Insert Covered Entity or Business Associate name] any necessary Privacy Policy Procedure changes.
4. Periodic Evaluation by [Insert Covered Entity or Business Associate name] Evaluation Team
   1. The Evaluation Team will include the Security Officer, the Privacy Officer, the Facility Office Manager, the Disaster Recovery Planner, and anyone else the facility deems necessary.
   2. The Evaluation Team will reconvene on an annual basis to evaluate the technical and non-technical viability of [Insert Covered Entity or Business Associate name] Security and Privacy Policies.
   3. Any member of the Evaluation Team, the Information Security Officer, or any other person may suggest changes to the Security or Privacy Policies or Procedures by submitting such suggestions to the Evaluation Team for consideration.
   4. The Evaluation Team will review any suggested Security or Privacy Policy or Procedure change(s) and make a preliminary recommendation.
   5. If the Evaluation Team preliminarily recommends a new security or privacy standard or a change in [Insert Covered Entity or Business Associate name] Security or Privacy Policies or Procedures, such new standard or change will be communicated to [Insert Covered Entity or Business Associate name] Departments by the Evaluation Team, who will elicit feedback for a specific period of time and provide such feedback to the Information Security or Privacy Officer.
   6. The Evaluation Team will consider the feedback received and make a final recommendation on the suggested change to the Information Security or Privacy Officer.
   7. If the Information Security or Privacy Officer approves the change, such change will be propagated to [Insert Covered Entity or Business Associate name] Departments through policy updates and reminders. [Insert Covered Entity or Business Associate name] will be required to update their Security or Privacy Procedure in a timely manner to incorporate the change.
   8. The Information Security or Privacy Officer will update the document, incorporating the updated policies and sign with the appropriate effective date.
5. Evaluation Upon Occurrence of Certain Events
   1. In the event that one or more of the following events occur, the policy evaluation process described in will be immediately triggered:
      1. Changes in the HIPAA Security Regulations or Privacy Regulations.
      2. New federal, state, or local laws or regulations affecting the privacy or security of PHI.
      3. Changes in technology, environmental processes or business processes that may affect HIPAA Security or Privacy Policies or Procedures.
      4. A serious security violation, breach, or other security incident occurs.
   2. The Information Security or Privacy Officer may reconvene the Evaluation Team if deemed necessary based on information received from, but not limited to, the HIPAA Security or Privacy Officer or an Internal Audit.
6. Evaluation of [Insert Covered Entity or Business Associate name] Procedures
   1. [Insert Covered Entity or Business Associate name] must periodically (at least annually) evaluate its HIPAA Security or Privacy Procedures to ensure that departments follow such Procedures and that these procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security or Privacy Policies.
7. Internal Audit of Security Policies and Procedures
   1. All HIPAA Security or Privacy Policies and [Insert Covered Entity or Business Associate name] Department procedures are subject to periodic audits by [Insert Covered Entity or Business Associate name] management and/or the Information Security or Privacy Officer.

**Violations:**

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.